PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-259621

(43)Date of publication of application : 13.09.2002

(51)Int.Cl. G06F 17/60
G09C 1/00
H04L 9/32

(21)Application number : 2001-052429

(22)Date of filing : 27.02.2001

(71)Applicant : NTT ADVANCED TECHNOLOGY CORP

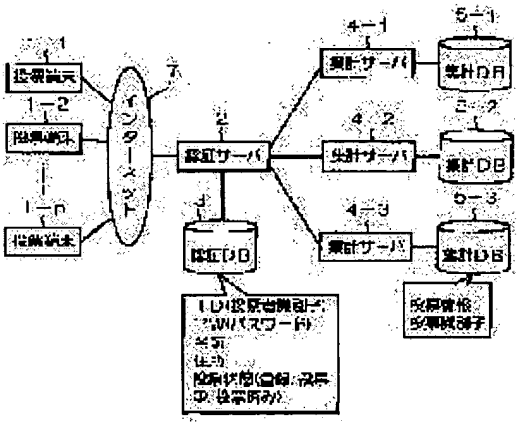
(72)Inventor : TANAKA TOSHIKIYO

(54) SYSTEM AND METHOD FOR ELECTRONIC VOTING

(57)Abstract:

PROBLEM TO BE SOLVED: To save the trouble and space to count votes, to eliminate invalid votes and questionable votes, and to prevent the votes from being miscounted.

SOLUTION: At voting terminals 1-1 to 1-n, voters vote by using touch panels. An authentication server 2 generates a blind signature in vote information to authenticate the voters. The voting terminals 1-1 to 1-n seal the vote information with double electronic envelopes by ciphering technology and send it to the authentication server 2 through the Internet 7. The authentication server 2 unseal the outside envelope and sends the information to three totaling servers 4-1 to 4-3. The totaling servers 4-1 to 4-3 unseal the inside envelope and total the votes according to the voting contents. After the votes are counted, the totaling servers 4-1 to 4-3 verify the voting results which are collected and totaled and if any discrepancy is found, correct values are determined through majority decision making.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－259621
（P2002－259621A）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
G06F 17/60	148	G06F 17/60	148	5J104
	154		154	
	502		502	
	510		510	
	512		512	

審査請求　未請求　請求項の数11　OL　（全 8 頁）　最終頁に続く

(21)出願番号　特願2001－52429(P2001－52429)

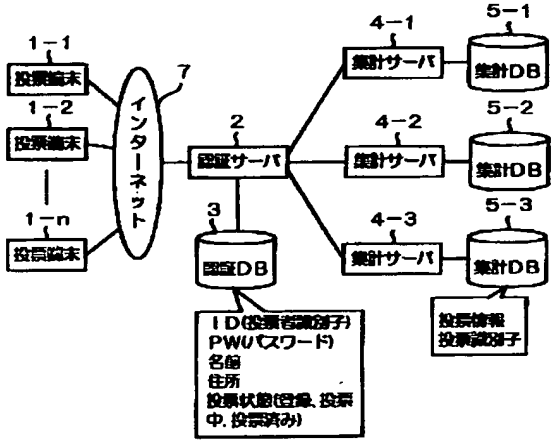
(22)出願日　平成13年２月27日(2001.2.27)

(71)出願人　000102739
エヌ・ティ・ティ・アドバンステクノロジ株式会社
東京都新宿区西新宿二丁目１番１号
(72)発明者　田中　利清
東京都新宿区西新宿二丁目１番１号　エヌ・ティ・ティ・アドバンステクノロジ株式会社内
(74)代理人　100064908
弁理士　志賀　正武

Ｆターム(参考)　5J104 AA07 AA09 AA16 EA06 EA19 KA01 LA08 MA01 NA05 NA35 NA41 PA17

(54)【発明の名称】　電子投票システムおよび電子投票方法

(57)【要約】
【課題】　人手の削減、開票スペースの縮小、無効票や疑問票の根絶、集計ミスの防止を実現する。
【解決手段】　投票端末１－１～１－ｎでは、投票者がタッチパネルを用いて投票する。認証サーバ２は、投票情報にブラインド署名を生成することで、投票者を認証する。投票端末１－１～１－ｎは、投票情報を暗号化技術により、２重の電子的封筒で密封してインターネット７を介して認証サーバ２に送る。認証サーバ２は、外側の封筒を開封し、３つの集計サーバ４－１～４－３へ送る。集計サーバ４－１～４－３は、各々、内側の封筒を開封し、投票内容に基づいて集計を行う。開票終了後、集計サーバ４－１～４－３が集票・集計した投票結果を照合し、不一致が見つかった場合には、多数決で正解値を決める。



1

【特許請求の範囲】

【請求項1】　ネットワークに接続され、投票者により候補者に対して行われる投票内容を暗号化し、暗号化投票内容を生成する投票端末と、

前記投票端末における前記投票者を、前記ネットワークを介して認証する認証装置と、

前記認証装置を介して前記投票端末からの暗号化投票内容を復号して投票内容を取得し、該投票内容に基づいて候補者の得票を集計する集計装置とを具備することを特徴とする電子投票システム。

【請求項2】　前記投票端末は、

投票者により行われた投票内容を暗号化して、第1の暗号化投票内容を生成する第1の暗号化手段と、

前記第1の暗号化手段により暗号化された第1の暗号化投票内容を暗号化して第2の暗号化投票内容を生成する第2の暗号化手段とを具備し、

前記認証装置は、

前記投票端末の前記第2の暗号化手段により暗号化された第2の暗号化投票内容を復号して前記第1の暗号化投票内容を取得する第1の復号化手段を具備し、前記集計装置は、

前記認証装置の前記第1の復号化手段により復号された第1の暗号化投票内容を復号して前記投票内容を取得する第2の復号化手段を具備することを特徴とする請求項1記載の電子投票システム。

【請求項3】　前記第1の暗号化手段は、

投票者により行われた投票内容を、第1の共通鍵を用いて暗号化し、該第1の共通鍵を、前記集計装置の第1の公開鍵を用いて暗号化し、

前記第2の暗号化手段は、

前記第1の暗号化投票内容を、第2の共通鍵を用いて暗号化し、該第2の共通鍵を、前記認証装置の第2の公開鍵を用いて暗号化し、

前記第1の復号化手段は、暗号化された第2の共通鍵を、前記第2の公開鍵に対応する第2の秘密鍵を用いて復号して前記第2の共通鍵を取得する第2の共通鍵復号手段と、復号された第2の共通鍵を用いて、前記第2の暗号化投票内容を復号して前記第1の暗号化投票内容を取得する第2の暗号化投票内容復号化手段とを備え、

前記第2の復号化手段は、暗号化された第1の共通鍵を、前記第1の公開鍵に対応する第1の秘密鍵を用いて復号して前記第1の共通鍵を取得する第1の共通鍵復号手段と、復号された第1の共通鍵を用いて、前記第1の暗号化投票内容を復号して前記投票内容を取得する第1の暗号化投票内容復号化手段とを備えることを特徴とする請求項2記載の電子投票システム。

【請求項4】　前記認証装置は、

投票者の正当性を認証すべく、前記投票端末により暗号化された投票内容に対してブラインド署名を生成するブラインド署名手段を備え、

2

前記投票端末は、

投票者により選択された候補者に対応する投票内容を暗号化し、前記認証装置に送信する第3の暗号化手段と、

前記認証装置のブラインド署名手段により生成されたブラインド署名から署名情報を取得する署名取得手段とを備えることを特徴とする請求項1ないし3のいずれかの記載の電子投票システム。

【請求項5】　前記集計装置は、

前記投票内容に対して識別情報を生成する識別情報生成手段と、

前記投票内容を前記識別情報とともに蓄積する蓄積手段とを具備することを特徴とする請求項1ないし4のいずれかの記載の電子投票システム。

【請求項6】　前記第1の公開鍵および第1の秘密鍵、ならびに前記第2の公開鍵および第2の秘密鍵は、各々、前記認証装置または前記集計装置に着脱可能な、外部へ情報が漏洩しないようにプロテクトされた、ICカード内で生成・管理されることを特徴とする請求項3ないし5のいずれかの記載の電子投票システム。

【請求項7】　ネットワークに接続された投票端末から投票者が投票し、

該投票された投票内容を暗号化して、前記ネットワークに接続された認証装置に送信し、

前記認証装置は、投票者の認証を行い、認証された場合は、前記暗号化された内容を前記集計装置に送信し、

前記集計装置によって前記暗号化投票内容を復号して投票内容を取得し、

該投票内容に基づいて候補者の得票を集計することを特徴とする電子投票方法。

【請求項8】　前記投票端末は、前記投票内容を暗号化して暗号化投票内容を生成し、

前記認証装置は、前記投票端末により暗号化された暗号化投票内容に対してブラインド署名を生成し、

前記投票端末は、前記ブラインド署名から署名情報を取得することを特徴とする請求項7記載の電子投票方法。

【請求項9】　前記投票内容の暗号化では、

前記投票者により行われた投票内容を、第1の共通鍵を用いて暗号化して前記第1の暗号化投票内容を生成し、

前記第1の共通鍵を、前記集計装置の第1の公開鍵を用いて暗号化し、

前記第1の暗号化投票内容を、第2の共通鍵を用いて暗号化して第2の暗号化投票内容を生成し、

前記第2の共通鍵を、前記認証装置の第2の公開鍵を用いて暗号化し、

前記暗号化投票内容の復号化では、

前記暗号化された第2の共通鍵を、前記第2の公開鍵に対応する第2の秘密鍵を用いて復号して前記第2の共通鍵を取得し、

前記復号された第2の共通鍵を用いて、前記第2の暗号化投票内容を復号して前記第1の暗号化投票内容を取得

し、
前記暗号化された第１の共通鍵を、前記第１の公開鍵に対応する第１の秘密鍵を用いて復号して前記第１の共通鍵を取得し、
前記復号された第１の共通鍵を用いて、前記第１の暗号化投票内容を復号して投票内容を取得することを特徴とする請求項７記載の電子投票方法。
【請求項１０】　前記投票内容に対して識別情報を生成し、前記投票内容を前記識別情報とともに蓄積することを特徴とする請求項７ないし９のいずれかに記載の電子投票方法。
【請求項１１】　前記第１の公開鍵および第１の秘密鍵、ならびに前記第２の公開鍵および第２の秘密鍵は、各々、認証装置または集計装置に着脱可能な、外部へ情報が漏洩しないようにプロテクトされた、ＩＣカード内で生成・管理されることを特徴とする請求項７ないし１０のいずれかに記載の電子投票方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、国政選挙や地方選挙などの投票に用いて好適な電子投票システムおよび電子投票方法に関する。
【０００２】
【従来の技術】従来より、国政選挙や地方選挙などの投票においては、有権者が投票所で、投票用紙に候補者氏名を書き込み、該投票用紙を集め、多くの人手で１枚ずつ投票用紙に書かれた候補者氏名を確認、カウントすることで行われてきた。
【０００３】
【発明が解決しようとする課題】しかしながら、上述した従来技術では、大量の人手や、開票スペースが必要である。また、投票者氏名は、投票者による手書きであるため、記入ミスによる無効票や疑問票が絶えない。また、人による目視確認であるため、集計ミスも起り得るという問題があった。
【０００４】この発明は上述した事情に鑑みてなされたもので、人手の削減、開票スペースの縮小、無効票や疑問票の根絶、集計ミスの防止を実現することができる電子投票システムおよび電子投票方法を提供することを目的とする。
【０００５】
【課題を解決するための手段】上述した問題点を解決するために、請求項１記載の発明では、ネットワークに接続され、投票者により候補者に対して行われる投票内容を暗号化し、暗号化投票内容を生成する投票端末と、前記投票端末における前記投票者を、前記ネットワークを介して認証する認証装置と、前記認証装置を介して前記投票端末からの暗号化投票内容を復号して投票内容を取得し、該投票内容に基づいて候補者の得票を集計する集計装置とを具備することを特徴とする。
【０００６】また、請求項２記載の発明では、請求項１記載の電子投票システムにおいて、前記投票端末は、投票者により行われた投票内容を暗号化して、第１の暗号化投票内容を生成する第１の暗号化手段と、前記第１の暗号化手段により暗号化された第１の暗号化投票内容を暗号化して第２の暗号化投票内容を生成する第２の暗号化手段とを具備し、前記認証装置は、前記投票端末の前記第２の暗号化手段により暗号化された第２の暗号化投票内容を復号して前記第１の暗号化投票内容を取得する第１の復号化手段を具備し、前記集計装置は、前記認証装置の前記第１の復号化手段により復号された第１の暗号化投票内容を復号して前記投票内容を取得する第２の復号化手段を具備することを特徴とする。
【０００７】また、請求項３記載の発明では、請求項２記載の電子投票システムにおいて、前記第１の暗号化手段は、投票者により行われた投票内容を、第１の共通鍵を用いて暗号化し、該第１の共通鍵を、前記集計装置の第１の公開鍵を用いて暗号化し、前記第２の暗号化手段は、前記第１の暗号化投票内容を、第２の共通鍵を用いて暗号化し、該第２の共通鍵を、前記認証装置の第２の公開鍵を用いて暗号化し、前記第１の復号化手段は、暗号化された第２の共通鍵を、前記第２の公開鍵に対応する第２の秘密鍵を用いて復号して前記第２の共通鍵を取得する第２の共通鍵復号手段と、復号された第２の共通鍵を用いて、前記第２の暗号化投票内容を復号して前記第１の暗号化投票内容を取得する第２の暗号化投票内容復号化手段とを備え、前記第２の復号化手段は、暗号化された第１の共通鍵を、前記第１の公開鍵に対応する第１の秘密鍵を用いて復号して前記第１の共通鍵を取得する第１の共通鍵復号手段と、復号された第１の共通鍵を用いて、前記第１の暗号化投票内容を復号して前記投票内容を取得する第１の暗号化投票内容復号化手段とを備えることを特徴とする。
【０００８】また、請求項４記載の発明では、請求項１ないし３のいずれかの記載の電子投票システムにおいて、前記認証装置は、投票者の正当性を認証すべく、前記投票端末により暗号化された投票内容に対してブラインド署名を生成するブラインド署名手段を備え、前記投票端末は、投票者により選択された候補者に対応する投票内容を暗号化し、前記認証装置に送信する第３の暗号化手段と、前記認証装置のブラインド署名手段により生成されたブラインド署名から署名情報を取得する署名取得手段とを備えることを特徴とする。
【０００９】また、請求項５記載の発明では、請求項１ないし４のいずれかの記載の電子投票システムにおいて、前記集計装置は、前記投票内容に対して識別情報を生成する識別情報生成手段と、前記投票内容を前記識別情報とともに蓄積する蓄積手段とを具備することを特徴とする。
【００１０】また、請求項６記載の発明では、請求項３

ないし５のいずれかの記載の電子投票システムにおいて、前記第１の公開鍵および第１の秘密鍵、ならびに前記第２の公開鍵および第２の秘密鍵は、各々、前記認証装置または前記集計装置に着脱可能な、外部へ情報が漏洩しないようにプロテクトされた、ＩＣカード内で生成・管理されることを特徴とする。

【００１１】上述した問題点を解決するために、請求項７記載の発明では、ネットワークに接続された投票端末から投票者が投票し、該投票された投票内容を暗号化して、前記ネットワークに接続された認証装置に送信し、前記認証装置は、投票者の認証を行い、認証された場合は、前記暗号化された内容を前記集計装置に送信し、前記集計装置によって前記暗号化投票内容を復号して投票内容を取得し、該投票内容に基づいて候補者の得票を集計することを特徴とする。

【００１２】また、請求項８記載の発明では、請求項７記載の電子投票方法において、前記投票端末は、前記投票内容を暗号化して暗号化投票内容を生成し、前記認証装置は、前記投票端末により暗号化された暗号化投票内容に対してブラインド署名を生成し、前記投票端末は、前記ブラインド署名から署名情報を取得することを特徴とする。

【００１３】また、請求項９記載の発明では、請求項７記載の電子投票方法において、前記投票内容の暗号化では、前記投票者により行われた投票内容を、第１の共通鍵を用いて暗号化して前記第１の暗号化投票内容を生成し、前記第１の共通鍵を、前記集計装置の第１の公開鍵を用いて暗号化し、前記第１の暗号化投票内容を、第２の共通鍵を用いて暗号化して第２の暗号化投票内容を生成し、前記第２の共通鍵を、前記認証装置の第２の公開鍵を用いて暗号化し、前記暗号化投票内容の復号化では、前記暗号化された第２の共通鍵を、前記第２の公開鍵に対応する第２の秘密鍵を用いて復号して前記第２の共通鍵を取得し、前記復号された第２の共通鍵を用いて、前記第２の暗号化投票内容を復号して前記第１の暗号化投票内容を取得し、前記暗号化された第１の共通鍵を、前記第１の公開鍵に対応する第１の秘密鍵を用いて復号して前記第１の共通鍵を取得し、前記復号された第１の共通鍵を用いて、前記第１の暗号化投票内容を復号して投票内容を取得することを特徴とする。

【００１４】また、請求項１０記載の発明では、請求項７ないし９のいずれかに記載の電子投票方法において、前記投票内容に対して識別情報を生成し、前記投票内容を前記識別情報とともに蓄積することを特徴とする。

【００１５】また、請求項１１記載の発明では、請求項７ないし１０のいずれかに記載の電子投票方法において、前記第１の公開鍵および第１の秘密鍵、ならびに前記第２の公開鍵および第２の秘密鍵は、各々、認証装置または集計装置に着脱可能な、外部へ情報が漏洩しないようにプロテクトされた、ＩＣカード内で生成・管理されることを特徴とする。

【００１６】この発明では、ネットワークに接続された投票端末から投票者が投票し、該投票された投票内容を、前記ネットワークに接続された認証装置により認証し、前記認証された投票内容を暗号化して、前記ネットワークを介して、前記認証装置に接続されている集計装置に送信し、前記集計装置によって前記暗号化投票内容を復号して投票内容を取得し、該投票内容に基づいて候補者の得票を集計する。したがって、人手の削減、開票スペースの縮小、無効票や疑問票の根絶、集計ミスの防止を実現することが可能となる。

【００１７】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。

Ａ．実施形態の構成

図１は、本発明の実施形態による電子投票システムの構成を示すブロック図である。図１において、投票端末１－１，１－２，…，１－ｎは、投票所に設置された端末であり、パーソナルコンピュータなどから構成されている。該投票端末１－１～１－ｎは、インターネット７に接続されている。投票端末１－１～１－ｎは、１つの投票所に複数台（ｎ台）設置されており、その設置台数は、投票所で投票する有権者の数に応じて定められている。

【００１８】上記投票端末１－１～１－ｎは、候補者情報を暗号化する機能、後述する認証サーバ２により生成されたディジタル署名を復号する機能（アンブラインド）、さらに、候補者情報とディジタル署名とに対して２重の暗号化を行う機能などを有する。これら機能（動作）については後述する。

【００１９】投票者は、投票端末１－１～１－ｎのタッチパネル上の数字ボタンをタッチすることで、投票者を認証するためのＩＤ（投票者識別子）やパスワード、候補者などを入力する。ＩＤ、パスワードは、例えば、図２に示すように、３桁毎のグループに分割し、各グループに番号を付ける。ＩＤ、パスワードは、高齢者等の投票者に考慮し、読み間違い、入力ミスを低減するために数字のみで構成することが好ましい。

【００２０】なお、投票端末１－１～１－ｎは、投票者の自宅に設置されてもよいが、この場合、所定の投票用ソフトウエアを予めインストールしておく必要がある。

【００２１】認証サーバ２は、インターネット７を介して投票端末１－１～１－ｎに対して、上記ＩＤ、パスワード、誕生日などを要求し、それら情報を照合して投票者を認証する。また、認証サーバ２は、インターネット７を介して投票端末１－１～１－ｎに対して、候補者情報（氏名、党名、顔写真）を送信し、投票端末１－１～１－ｎからの投票情報（暗号化済）にディジタル署名（ブラインド署名）を発行する。また、認証サーバ２は、投票端末１－１～１－ｎからの暗号化された投票情

報を、後述する3台の集計サーバ4－1，4－2，4－3に送信するようになっている。また、認証サーバ2は、投票者の認証を行ったり、投票状態を管理したりするための認証データベース3を備えている。該認証データベース3は、投票者毎のＩＤ、パスワード、名前、住所、投票状態（登録、投票中、投票済み）を蓄積している。

【００２２】集計サーバ4－1～4－3は、それぞれが物理的に隔離され、同一の機能を有する3つのサーバからなる。集計サーバ4－1～4－3は、各々、それぞれ独立に集票および集計を行う。より具体的には、集計サーバ4－1～4－3は、各々、認証サーバ2からの投票情報に対して、認証サーバ2によるディジタル署名を検証し、投票識別子を生成・付加し、集計データベース5－1，5－2，5－3に格納する。それぞれの集計サーバ4－1～4－3による集計結果は、互いに照合され、不一致が見つかった場合には、多数決で正解値を決めるようになっている。

【００２３】なお、上述した認証サーバ2および集計サーバ4－1～4－3では、投票情報の暗号化と復号およびディジタル署名を行うようになっているが、該暗号化と復号およびディジタル署名において用いられる、秘密鍵の生成と復号、および署名生成は、ＩＣカードなどの記憶媒体内で実施されるようになっている。秘密鍵は、ＩＣカードから読み出せないようにプロテクトされている。このため、紛失等に対応したバックアップができないので、秘密鍵の種類の数（この例では2、集計サーバの場合には3種類）だけ署名および暗号化を行い、冗長化している。

【００２４】Ｂ．実施形態の動作次に、図3に示すフローチャートを参照して本実施形態の動作について詳細に説明する。ここで、図4は、認証サーバからディジタル署名を得る過程を示すフローチャートである。また、図5は、上記投票端末での密封、認証サーバでの開封、集計サーバでの開封の様子を示す概念図である。

【００２５】投票者は、予め自宅の端末からインターネットを介して認証サーバにアクセスし、認証サーバが提示する選挙管理Ｗｅｂ画面から個人情報（名前、住所など）を登録する（ステップＳ１）。認証サーバ2は、登録した投票者に対してＩＤ（投票者識別子）、ＰＷ（パスワード）が記入されたシール付きはがき（投票整理券）を自宅に郵送する（ステップＳ２）。なお、自宅に端末を所持しない有権者も居るので、現行通り、認証サーバ2（所轄役所）側から自動的に有権者に対してシール付きはがき（投票整理券）を自宅に郵送するようにしてもよい。

【００２６】次に、投票日になると、投票者は自宅の端末から投票を行う。自宅に端末を持たない投票者は自宅に郵送された投票整理券を持参して投票所に出向き、投票所の端末から投票を行う。投票者は、自宅又は投票所に設置された、投票端末1－ｉ（ｉ＝1～ｎ）から投票を開始する（ステップＳ３）。

【００２７】認証サーバ2は、インターネット7を介して、上記投票端末1－ｉに対してＩＤ、パスワードおよび誕生日の入力を要求する（ステップＳ４）。投票者は、投票端末1－ｉのタッチパネルから、自宅に郵送されたシール付きはがきに印字されたＩＤ、パスワード、および誕生日（ＭＭＤＤ）を入力する（ステップＳ５）。ＩＤ、パスワードは、インターネット7を介して認証サーバ2に送信される。

【００２８】認証サーバ2は、上記投票端末1－ｉから入力された、ＩＤ、パスワード、および誕生日を、認証データベース3の情報と照合し、正しい投票者であるか、すなわち有権者であるか、二重投票ではないかなどをチェックする（ステップＳ６）。投票者が正当と認証された場合は、認証サーバ2は、候補者情報（氏名、党名、顔写真など）を、インターネット7を介して上記投票端末1－ｉに送信する（ステップＳ７）。投票者が正当と認証されなかった場合は、その旨を投票端末1－ｉに表示し、当該投票者への処理を中止する。

【００２９】投票者は、投票端末1－ｉに表示される候補者情報を確認して候補者を選択（投票）する（ステップＳ８）。投票端末1－ｉでは、図4に示すように、選択された候補者の情報（以下、投票情報）をブラインド（暗号化）し、インターネット7を介して認証サーバ2に送信する（ステップＳ９）。認証サーバ2では、図4に示すように、上記暗号化された投票情報に対してディジタル署名（ブラインド署名）を生成し、インターネット7を介して、投票端末1－ｉに送信する（ステップＳ１０）。投票端末1－ｉでは、図4に示すように、上記ブラインド署名をアンブラインド（復号）し、ディジタル署名を取得する（ステップＳ１１）。このように、ブラインド署名を用いることで、認証サーバ2では、投票者を特定できるが、投票内容を知ることはできない（匿名性の保証）。そして、認証サーバにより、その投票者が本人であること、その投票内容が投票者本人によるものであること、票が重複して投じられていないことが認証されることになる。

【００３０】次にブラインド署名の方式の例を示す。認証サーバの秘密鍵をｄ、公開鍵をｅ、ｎ、投票情報をｍとする。また以下の演算はｎの剰余の基での演算である。投票端末は、乱数ｒを生成し、ｒのｅ乗とｍの積をｘとして認証サーバへ送付する。認証サーバはｘのｄ乗をｙとして投票端末へ送付する。このｙがブラインド署名である。投票端末はｙをｒで除算する。ｄ＝1／ｅであるので、除算結果はｍのｄ乗となり、これはｍに対する署名そのものである。

【００３１】次に、投票端末1－ｉでは、図5に示すように、上記投票情報（ディジタル署名を含む）を封筒Ａにより密封した後（ステップＳ１２）、さらに、封筒Ｂ

により密封し（ステップＳ１３）、インターネット７を介して認証サーバ２へ送信する。認証サーバ２では、図５に示すように、外側の封筒Ｂのみを開封し（ステップＳ１４）、集計サーバ４－１～４－３に送信する。集計サーバ４－１～４－３では、図５に示すように、封筒Ａを開封し（ステップＳ１５）、元の投票情報（ディジタル署名を含む）を取得する。

【００３２】以下に、上記投票端末１－１～１－ｎでの密封、認証サーバ２での開封、集計サーバ４－１～４－３での開封についてより詳細に説明する。ここで、図６は、上記投票端末での密封の詳細な様子を示す概念図である。また、図７は、上記認証サーバおよび集計サーバでの開封の詳細な様子を示す概念図である。

【００３３】投票端末１－１～１－ｎでは、図６に示すように、上記投票情報（ディジタル署名を含む）を共通鍵ＫＡ１で暗号化することにより（ステップＳａ１）、封筒Ａにより密封した後、上記共通鍵ＫＡ１を、集計サーバ４－ｉ（ｉ＝１，２，３）が公開している公開鍵ＫＢ１により暗号化する（ステップＳａ２）。次に、暗号化した投票情報（封筒Ａ）を、さらに、共通鍵ＫＡ２で暗号化することにより（ステップＳａ３）、封筒Ｂにより密封した後、上記共通鍵ＫＡ２を、認証サーバ２が公開している公開鍵ＫＢ２により暗号化する（ステップＳａ４）。これにより、投票情報は、封筒Ａ（内側）と封筒Ｂ（外側）で二重に密封（暗号化）されたことになる。該二重に暗号化された投票情報は、インターネット７を介して認証サーバ２へ送信される。

【００３４】認証サーバ２では、図７（ａ）に示すように、上記公開鍵ＫＢ２に対応する秘密鍵ＫＣ２により、暗号化された共通鍵ＫＡ２を復号して上記共通鍵ＫＡ２を取得し（ステップＳｂ１）、該共通鍵ＫＡ２で、上記二重に暗号化された投票情報（内側：封筒Ａ、外側：封筒Ｂ）を復号することで、外側の封筒Ｂを開封する（ステップＳｂ２）。そして、封筒Ａで密封された投票情報を集計サーバ４－１～４－３に送信する。

【００３５】集計サーバ４－ｉ（ｉ＝１，２，３）では、図７（ｂ）に示すように、上記公開鍵ＫＢ１に対応する秘密鍵ＫＣ１により、暗号化された共通鍵ＫＡ１を復号して共通鍵ＫＡ１を取得し（ステップＳｃ１）、該共通鍵ＫＡ１で、上記投票情報（封筒Ａ）を復号することで、封筒Ａを開封する（ステップＳｃ２）。この時点で、集計サーバ４－ｉには、元の投票情報（ディジタル署名を含む）が取得される。

【００３６】なお、上述した説明において、本実施形態では、３つの集計サーバ４－１～４－３を用いているので、実際には、集計サーバ毎に、それぞれの秘密鍵ＫＣ１－１，ＫＣ１－２，ＫＣ１－３と、該秘密鍵に対応する公開鍵ＫＢ１－１，ＫＢ１－２，ＫＢ１－３とを生成している。そして、投票端末１－ｉにおいて、投票情報を封筒Ａで密封する際には、共通鍵ＫＡ１を、上記公開鍵ＫＢ１－１，ＫＢ１－２，ＫＢ１－３の各々で暗号化している。

【００３７】図３に説明を戻すと、次に、集計サーバ４－１～４－３では、ディジタル署名に基づいて認証サーバ署名を検証し、認証サーバ２により認証された投票情報であるか否かをチェックする（ステップＳ１６）。次に、集計サーバ４－１～４－３は、例えばその時点における日時分秒ミリ秒マイクロ秒のデータのハッシュ値をとることで識別子を生成し（ステップＳ１７）、投票情報に付加して集計データベース５－１～５－３へ格納するとともに、投票情報に基づいて投票を集計する。開票終了後、集計サーバ４－１～４－３の各々において、それぞれ独立に集票・集計した投票結果を照合し、不一致が見つかった場合には、多数決で正解値を決める。

【００３８】

【発明の効果】以上説明したように、本発明によれば、ネットワークに接続された投票端末から投票者が投票し、該投票された投票内容を、前記ネットワークに接続された認証装置により認証し、前記認証された投票内容を暗号化して、前記ネットワークを介して、前記認証装置に接続されている集計装置に送信し、前記集計装置によって前記暗号化投票内容を復号して投票内容を取得し、該投票内容に基づいて候補者の得票を集計するようにしたので、人手の削減、開票スペースの縮小、無効票や疑問票の根絶、集計ミスの防止を実現することができるという利点が得られる。

【図面の簡単な説明】

【図１】　本発明の実施形態による電子投票システムの構成を示すブロック図である。

【図２】　本実施形態による投票者のＩＤ、パスワードの構成を示す概念図である。

【図３】　本発明の実施形態による電子投票システムの動作を説明するためのフローチャートである。

【図４】　認証サーバからディジタル署名を得る過程を示すフローチャートである。

【図５】　投票端末での密封、認証サーバでの開封、集計サーバでの開封の様子を示す概念図である。

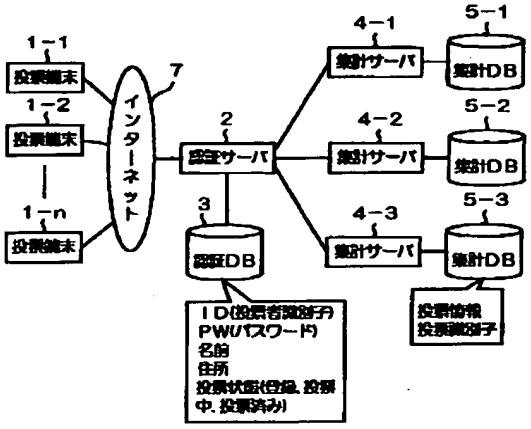
【図６】　投票端末での密封の詳細な様子を示す概念図である。

【図７】　認証サーバでおよび集計サーバでの開封の詳細な様子を示す概念図である。

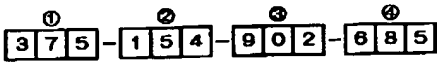
【符号の説明】

１－１～１－ｎ　投票端末
２　認証サーバ（認証装置）
３　認証データベース
４－１～４－３　集計サーバ（集計装置）
５－１～５－３　集計データベース
７　インターネット

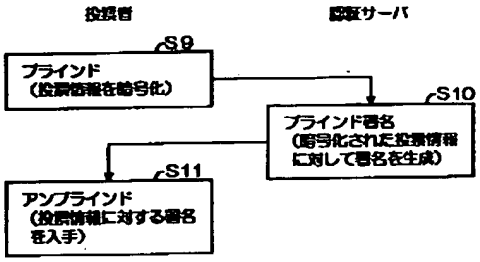
【図1】


1-1
投票端末
1-2
投票端末
1-n
投票端末
インターネット
7
2
認証サーバ
3
認証DB
4-1
集計サーバ
4-2
集計サーバ
4-3
集計サーバ
5-1
集計DB
5-2
集計DB
5-3
集計DB
ID(投票者識別子)
PW(パスワード)
名前
住所
投票状態(投票前, 投票中, 投票済み)
投票情報
投票識別子

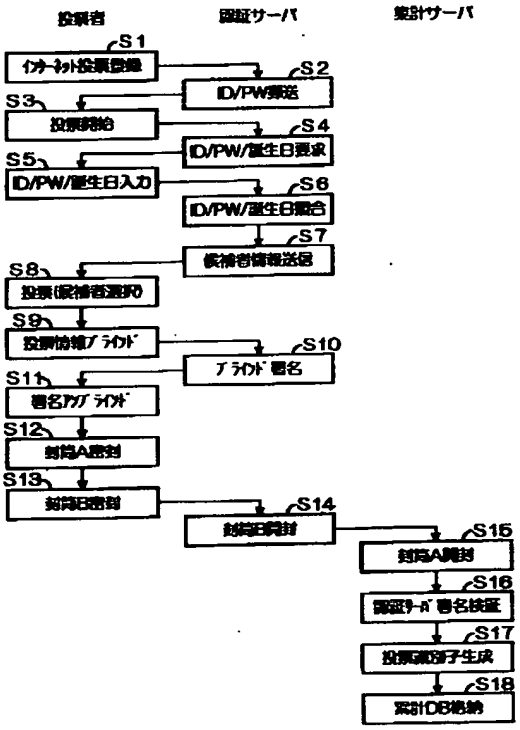
【図2】


①
②
③
④
3 7 5 - 1 5 4 - 9 0 2 - 6 8 5

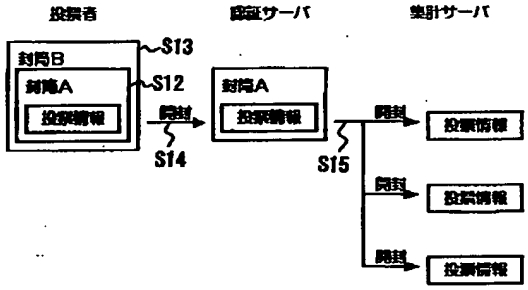
【図4】


投票者
認証サーバ
S9
ブラインド
(投票情報を暗号化)
S10
ブラインド署名
(暗号化された投票情報に対して署名を生成)
S11
アンブラインド
(投票情報に対する署名を入手)

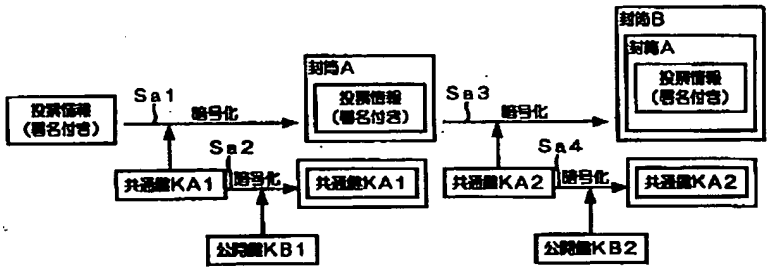
【図3】


投票者
認証サーバ
集計サーバ
S1
S2
ID/PW要求
S3
投票開始
S4
ID/PW/誕生日要求
S5
ID/PW/誕生日入力
S6
ID/PW/誕生日照合
S7
候補者情報送信
S8
S9
S10
ブラインド署名
S11
S12
封筒A開封
S13
S14
S15
封筒A開封
S16
S17
S18

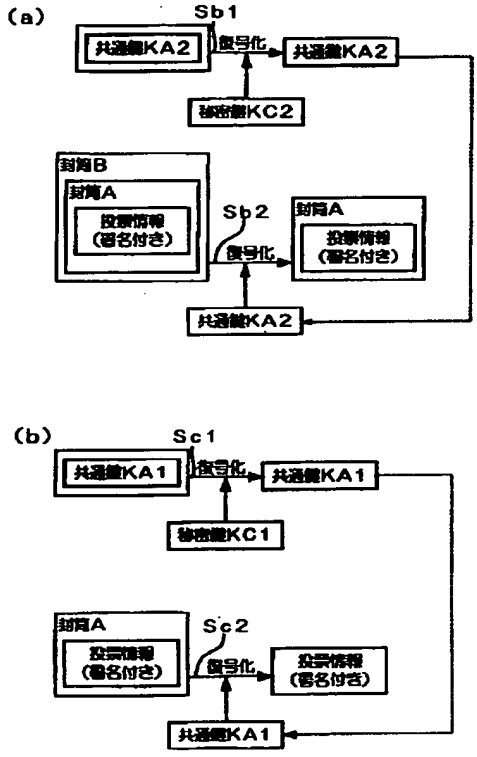
【図5】


投票者
認証サーバ
集計サーバ
封筒B
封筒A
投票情報
S13
S12
開封
S14
封筒A
投票情報
S15
開封
投票情報
開封
投票情報
開封
投票情報

【図6】



【図7】



フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
G09C	1/00	660	G09C	1/00	660Z
H04L	9/32		H04L	9/00	673A
					675B